МИНИСТЕРСТВО НА ОБРАЗОВАНИЕТО И НАУКАТА
ЦЕНТЪР ЗА СПЕЦИАЛНА ОБРАЗОВАТЕЛНА ПОДКРЕПА „Св. Св. Кирил и Методий“

с.Кривня, общ.Провадия, обл.Варна, тел., 0878273413,
e-mail: info400162@edu.mon.bg; csop_metodii@abv.bg

Утвърждавам:.....,
Директор – Ив. Богданова

ВЪТРЕШНИ ПРАВИЛА

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

НА ЦЕНТЪР ЗА СПЕЦИАЛНА ОБРАЗОВАТЕЛНА ПОДКРЕПА

„СВЕТИ СВЕТИ КИРИЛ И МЕТОДИЙ“ С. КРИВНЯ

Учебна 2026- 2027 г

Настоящите вътрешни правила се издават от Директора на центъра на основание Регламент (ЕС) 2016/679 и Закона за защита на личните данни (ЗЗЛД), утвърдени със Заповед

РАЗДЕЛ. 1

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Център за специална образователна подкрепа“ Св. св Кирил и Методий“ с. Кривня (ЦСОП) е държавна образователна институция в системата на предучилищното и училищното образование и е юридическо лице със седалище с. Кривня , п.к. 9217, ул. Първа № 1, с номер по Булстат/ЕИК 000086985. Основен предмет на дейност на центъра е: учебно – възпитателна и терапевтична дейност с ученици със специални образователни потребности (СОП) в задължителна предучилищна и училищна възраст. Центърът функционира във връзка и взаимодействие с другите институции в системата на предучилищното и училищното образование, със специализирани институции за деца, със социални услуги, с лечебни заведения и с родителите. Центърът осъществява диагностична, рехабилитационна, корекционно – терапевтична и обучителна функция в областта на обучението и подкрепата за личностно развитие на децата и учениците със специални образователни потребности.

Чл.2. Центърът се ръководи, управлява и представлява от директор. При управлението на дейността на центъра директорът се подпомага от заместник – директори. Заместник –директор по учебна дейност подпомага директора при управлението и контрола на образователната и терапевтична дейност в центъра. В центъра работят още счетоводител/ по чл.107 от КТ/, ЗАТС – касиер-домакин, учители – специални педагози, учители по специалности за професионално обучение, психолог, логопед, рехабилитатор - медицинско лице, учители ЦДО, възпитатели и други специалисти и служители при необходимост.

Чл.3. Центърът води и съхранява задължителните документи в съответствие с държавния образователен стандарт и изискванията на Закона за предучилищното и училищното образование, Наредба № 8 от 11.08.2016г. за информацията и документите за системата на предучилищното и училищното образование, Наредбата за приобщаващо образование от 17.10.2017 г. и другите нормативни актове, касаещи насочването, записването и дейността в центъра.

Чл.4. Центърът е администратор на лични данни по смисъла на чл. 4 пар. 7 от Регламент (ЕС) 2016/679 на Европейския Парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни (General Data Protection Regulation или GDPR). Центърът обработва лични данни във връзка със своята дейност и за нейните цели.

Чл.5. Настоящите вътрешни правила уреждат организацията на обработване и защитата на лични данни на всички служители и специалисти в центъра, обучаемите (ученици), родителите, посетителите, както и на други физически лица, свързани с осъществяването на дейността на центъра. Целта на настоящите вътрешни правила е установяването на ясни правила при събиране, обработка, съхраняване и предоставяне на лични данни от водените от центъра регистри, за да се гарантира неприкосновеността на личността и личния живот и да се защитят физическите лица от неправомерно обработване на свързаните с тях лични данни.

Чл.6. Вътрешните правила се приемат с цел да регламентират:

- **създаването на процедури и механизми** за гарантиране на неприкосновеността на личността и личния живот чрез осигуряване на защита на физическите лица в процеса на обработване на свързаните с тях лични данни;
- **необходимите организационни и технически мерки** за защита на физическите лица във връзка с обработване на свързаните с тях лични данни, включително защита от

неправомерен достъп, изменение или разпространение, случайно или незаконно унищожаване, случайна загуба, както и от всички други форми на неправомерно обработване на лични данни;

- **правата и задълженията на длъжностните лица, обработващи лични данни** и/или имащи достъп до лични данни и тяхната отговорност при неизпълнение на задълженията им;
- **правата на физическите лица** – субекти на лични данни и реда и начина за упражняване на правата им.

Чл.7. Вътрешните правила се утвърждават, допълват, изменят и отменят от директора на ЦСОП„ Св. св Кирил и Методий“ . Вътрешните правила се довеждат до знанието на всички служители в центъра, обработващи лични данни и/или имащи достъп до лични данни, срещу подпис, за да се осигури тяхната осведоменост и отговорност за внедряване и приложение на правилата в цялостната дейност на центъра.

РАЗДЕЛ. 2

ЗАПОЗНАВАНЕ С ИЗИСКВАНИЯТА НА РЕГЛАМЕНТ (ЕС) 2016/679

Чл.8. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета на ЕС за защитата на физическите лица във връзка с обработването на лични данни (GDPR) е общ европейски закон, който се прилага автоматично и в Република България от 25 май 2018г. GDPR разширява правата на субектите на данни и въвежда редица нови задължения за администраторите и обработващите лични данни. Защитата на физическите лица във връзка с обработването на лични данни е основно право и всеки има право на защита и на контрол върху собствените му лични данни. Защитата, предоставена с новия общ Регламент се прилага само спрямо физическите лица във връзка с обработването на техните лични данни.

Чл.9. За целите на Регламента:

1/„лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“). Физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

2/ „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

3/ „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

4/ „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

5/ „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни;

6/ „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

7/ „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

8/ „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

Чл.10. Защитата на физическите лица се прилага за обработването на лични данни както с автоматични средства, така и за ръчното им обработване. Основните правила, свързани с обработването на лични данни, са следните:

- Лични данни на физически лица се събират и обработват единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства.
- Лични данни се събират и обработват за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, несъвместим с тези цели, или за други цели.
- Лични данни се събират и обработват в необходимия минимум, подходящ и достатъчен за целите на обработването.
- Личните данни се поддържат в точен и актуален вид. Предприемат се необходимите и навременни мерки за тяхното коригиране и/или за изтриване на неточни лични данни.

Чл.11. При събиране и обработване на лични данни следва да се спазват следните основни принципи:

- **Законосъобразност, добросъвестност и прозрачност**

Личните данни следва да се събират и обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните.

За да бъде обработването **законосъобразно**, личните данни следва да бъдат обработвани въз основа на съгласието на съответния субект на данни или на друго легитимно основание, установено по законодателен път, включващо необходимостта от изпълнение на договор, по който субектът на данни е страна или с оглед предприемане на стъпки по искане на субекта на данни преди встъпване в договорни отношения. Така регламентът определя, че обработването на лични данни е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

1/ субектът на данните е дал **съгласие за обработване** на личните му данни за една или повече конкретни цели.

Когато събирането и обработването се извършва въз основа на съгласието на субекта на данните, администраторът следва да може да докаже, че субектът на данните е дал съгласието си за операцията по обработване. Съгласие следва да се дава чрез ясно утвърдителен акт, с който да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни, например чрез

декларация за съгласие. Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне.

2/ обработването е **необходимо за изпълнението на договор**, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор.

Обработването на лични данни е законосъобразно, когато то е необходимо за сключване или изпълнение на договор или при намерение за сключване на договор, когато тези договорни отношения не могат да се осъществят при непредоставяне на личните данни. В такъв случай личните данни се предоставят и обработват само за конкретните цели (осъществяване на договорните отношения) и се съхраняват само за конкретен срок (до приключване изпълнението на договора).

3/ обработването е **необходимо за изпълнение/спазване на нормативно задължение**, което се прилага спрямо администратора;

4/ обработването на лични данни следва да се счита за законосъобразно и когато то е необходимо за да се защити интерес от първостепенно значение за живота на субекта на данните или жизненоважен интерес на друго физическо лице.

Принципите на **добросъвестно и прозрачно** обработване изискват субектът на данни да бъде информиран за съществуването на операция по обработване, както и за нейните цели. За физическите лица следва да е прозрачно по какъв начин и в какъв обхват отнасящи се до тях лични данни се събират, съхраняват и обработват.

При събиране на лични данни от субекта на данните, администраторът предоставя на субекта следната информация:

1/ данните, които идентифицират администратора, координатите за връзка с неговите представители;

2/ целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

3/ получателите или категориите получатели на личните данни;

4/ срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

5/ информация за правата на субекта: правото да изиска от администратора достъп, коригиране или изтриване на личните му данни; правото да иска ограничаване на обработването, правото да направи възражение срещу обработването, правото на преносимост на данните и правото на жалба до надзорен орган;

6/ дали предоставянето на лични данни е задължително или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и евентуалните последствия, ако тези данни не бъдат предоставени;

- **Ограничение на целите**

Личните данни следва да се събират за конкретни, изрично указани и легитимни цели и да не се обработват по-нататък по начин, несъвместим с тези цели.

❖ **Свеждане на данните до минимум**

Личните данни следва да се събират по начин подходящ, пряко относим и ограничен до необходимия минимум във връзка с целите, за които се събират и обработват. Обработването на лични данни следва да се сведе до минимум в съответствие с принципите на пропорционалност и необходимост.

❖ **Точност**

Личните данни следва да са точни и поддържани в актуален вид; при необходимост следва да се предприемат всички разумни мерки, за да се гарантира своевременното коригиране, актуализиране или изтриване на неточни лични данни, като се имат предвид целите, за които те се обработват.

❖ **Ограничение на съхранението**

Личните данни следва да са съхранявани във форма, която да позволява идентифицирането на субекта на данните и само за период, не по-дълъг от необходимото за конкретните цели, за които се обработват тези данни. С цел да се гарантира, че срокът на съхранение на личните данни не е по-дълъг от необходимия, администраторът следва да установи срокове за изтриване на данните или за техния периодичен преглед.

❖ **Цялостност и поверителност**

Личните данни следва да са обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

❖ **Отчетност**

Администраторът носи отговорност и следва да е в състояние да докаже спазването на всички принципи, свързани с обработването на лични данни.

Чл.12. ЦСОП„ Св. св Кирил и Методий“ прилага адекватна защита на личните данни, съобразена с нивото на нейното въздействие. Защитата включва:

❖ **Физическа защита**

Физическата защита в центъра се осигурява чрез набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп и защита на сградите и помещенията, в които се съхраняват и обработват лични данни. Основните **организационни мерки** включват определяне на помещенията, в които: (1) ще се съхраняват досиетата с документи, съдържащи лични данни; (2) ще се извършва обработката на личните данни; (3) ще се разполагат елементите на комуникационно – информационните системи за обработка на данни, като по отношение на тези помещения се прилагат подходящи организационни и технически мерки по защита и ограничаване на физическия достъп. Достъпът до тези помещения е контролиран и ограничен само за конкретни служители с оглед изпълнение на служебните им задължения, за които този достъп е необходим. Ограничаването на достъпа и безопасността се осигуряват посредством подходящи **технически мерки** за сигурност като: заключващи системи, използване на метални каси и шкафове, оборудване на помещенията с пожарогасителни средства,

осигуряване на електронните устройства с уникални потребителски идентификатори и пароли, инсталиране на системи за видеонаблюдение и др.

ЦСОП„ Св. св Кирил и Методий“ е въвело контрол на достъпа до сградата посредством видеонаблюдение . В сградата се допускат лица след представяне на документ за самоличност и изясняване на причината за посещението. Сградата и нейните прилежащи зони са снабдени със система за видеонаблюдение, като периодично се проверява и изпитва изправността и правилното функциониране на всички нейни елементи. Дейностите и правилата при събиране, съхранение и обработване на лични данни посредством видеонаблюдение са подробно описани в **Процедура по обработване, съхранение и защита на лични данни при видеонаблюдение в ЦСОП„ Св. св Кирил и Методий“** , представляваща приложение към настоящия правилник.

Компютрите и другите технически средства в Центъра, служещи за обработка и съхранение на лични данни, се държат в сградата и се изнасят само по изключение - при необходимост от изпълнение на домашна работа или по време на командировка. Компютрите са снабдени с пароли и ключове за достъп, лични акаунти на служителите и др. средства, гарантиращи ограничаване достъпът до базата данни в компютъра/ устройството само за конкретния служител, на когото устройството е предоставено за ползване.

❖ Персонална защита

Персоналната защита представлява система от организационни мерки спрямо физическите лица, които обработват лични данни по указание на администратора. Основни мерки за персонална защита са:

- Познаване на нормативната уредба в областта на защитата на личните данни;
- Познаване на политиките и вътрешните правила на организацията в областта на защитата на личните данни;
- Познаване на опасностите, свързани с нерегламентирано обработване на лични данни;

Мерките за персонална защита гарантират достъпа до лични данни само на лица, чиито служебни задължения или конкретно възложени задачи налагат такъв достъп, при спазване на принципа „Необходимост да знае“. Физическите лица, които обработват лични данни в Центъра, се запознават детайлно с настоящия правилник и с изискванията на Регламента (GDPR), като имат право да получават допълнителни разяснения и методически насоки.

❖ Документална защита

Основните приложими мерки за документална защита на личните данни са:

- *Определяне на регистрите, които ще се поддържат на хартиен носител*: на хартиен носител се съхраняват всички лични данни, които се попълват върху утвърдени бланкови документи и/или формуляри, свързани с изпълнение на действащите нормативни актове или пряко свързани с осъществяване на дейността на центъра.
- *Определяне на условията за събиране и обработване на лични данни*: лични данни се събират само с конкретна цел, пряко свързана с изпълнение на законовите задължения и/или нормалната дейност в центъра, а начинът на тяхното съхранение се съобразява със специфичните нужди за обработка.
- *Регламентиране на достъпа до регистрите*: достъпът до регистрите е ограничен и се предоставя само на оправомощени служители, при спазване на принципа „Необходимост да знае“.

- *Определяне на срокове за съхранение*: Личните данни се съхраняват толкова дълго, колкото е необходимо за целта, за която са били събрани, и/или за период съобразно изискванията на действащото законодателство.
- *Процедури за унищожаване*: Документи, съдържащи лични данни, които не подлежат на предаване в държавен архив, след изтичане на законовите срокове за тяхното съхранение и ако те не са необходими за нормалното функциониране на центъра, се унищожават по подходящ и сигурен начин (напр. нарязване с шредер, изгаряне, електронно изтриване и др. методи).

❖ **Защита на автоматизирани информационни системи и/или мрежи**

Защитата на автоматизираните информационни системи и/или мрежи в центъра включва набор от приложими технически и организационни мерки за предотвратяване на нерегламентиран достъп до системите и/или мрежите, в които се създават, обработват и съхраняват лични данни.

Основните мерки за защита на автоматизираните информационни системи и/или мрежи, обработващи лични данни, оценени с ниско ниво на въздействие, включват:

- Идентификация чрез използване на пароли за достъп до мрежата и ресурсите на центъра (вкл. смяна на паролите на определен период от време за повишаване на сигурността);
- Ограничаване на достъпа до регистрите единствено до лица, които са пряко натоварени или ангажирани със създаване, попълване, обработка, актуализация и поддръжка на регистрите;
- Защита от вируси, включително използване на стандартни конфигурации за компютърна и/или мрежова платформа;
- Използване само на софтуерни продукти с уредени авторски права, респ. контрол и поддръжка на софтуера;
- Политика за създаване и поддържане на резервни копия за възстановяване (back – up) за предотвратяване на загубата на информация и лични данни, което би затруднило нормалното функциониране на центъра;
- Използване на хардуер (сървъри) за съхранение и обработване на лични данни, отговарящ на съвременните изисквания и възможности за архивиране и възстановяване на данните и работното състояние на средата;
- Подписване на служебни документи и кореспонденция с универсален електронен подпис (УЕП) само от служителите, които са оправомощени, без право да се предоставя издаденият УЕП на трети лица.

ЦСОП„ Св. св Кирил и Методий“ ползва услугите на специализирано дружество за поддръжка на компютърната техника и информационните системи, осигурени във връзка с дейността.

❖ **Псевдонимизация**

Чл.13. Поддържаните регистри с лични данни в ЦСОП„ Св. св Кирил и Методий“ са:

- Регистър „Ученици“
- Регистър „Родители“
- Регистър „Договори с контрагенти и доставчици“
- Регистър „Трудови досиета“
- Регистър „Трудови и граждански договори“
- Регистър „Човешки ресурси“
- Регистър „Счетоводни документи“

- Регистър „Архив“
- Регистър „Заповеди“
- Регистър „Входяща и изходяща кореспонденция“
- Регистър „Проекти и обществени поръчки“
- Регистър “Трудови злополуки“
- Регистър „Видеонаблюдение“

Регистрите набират и съхраняват лични данни на ЦСОП„ Св. св Кирил и Методий“ оперативно с оглед изпълняване на образователно – възпитателния и терапевтичен процес, спазване на трудовото законодателство, спазване на Закона за счетоводството и другата приложима нормативна база. Формите на водене на регистрите биват: на хартиен и на електронен носител.

Директорът на центъра определя кой/кои служители отговарят и обработват всеки отделен регистър. За всеки регистър се оценява рискът от загубата или неправомерното обработване на съдържащите се в него лични данни според възможните вредни последствия, по следния начин: „ниско ниво на риска“, „средно ниво на риска“, „високо ниво на риска“, „изключително високо ниво на риска“, в съответствие с нормативно определените критерии залегнали в Регламента. При „изключително високо ниво на риска“, констатирано при условията на предходното изречение, се извършва „Оценка на въздействието“ спрямо критериите, залегнали в Регламент (ЕС) 2016/679.

Местонахождение на картотечните шкафове:

- За досиетата на учениците – в кабинет „ Дирекция“; „ Архив“;
- За досиетата на персонала – в кабинет „Канцелария “; „ Архив“;
- За договори, обществени поръчки, заповеди, входяща и изходяща кореспонденция – в кабинет на Директора и „канцелария“;
- За видеонаблюдение - в кабинет на Директора; и „ Канцелария“;

Лицата, отговарящи за водене и съхранение на данните в конкретен регистър, извършват действията по събиране, обработване, съхраняване и актуализация на личните данни в регистъра. Периодично, поне веднъж годишно, както и винаги при необходимост, личните данни в регистъра следва да се актуализират от лицето, обработващо данните, както и да се прави преценка относно архивиране на данните на технически носител.

Чл.14. Права и задължения на лицата, работещи с лични данни:

❖ Длъжностното лице по защита на данните е длъжно:
- Да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на Регламента и на националното законодателство в тази насока;
- Да участва в повишаването на осведомеността и обучението на персонала, участващ в операциите по събиране и обработване на лични данни;
- При поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните;
- Да дава становища и да консултира администратора и обработващите лични данни по всички въпроси, свързани със защитата на личните данни;
- Да дава насоки по спазването на Регламента и другите нормативни актове за защита на личните данни от администратора и обработващите лични данни;

- Да участва в заседания на ръководството, когато се обсъждат въпроси от областта на защитата на личните данни;
- Да си сътрудничи с надзорния орган;
- Да бъде точка за контакт за надзорния орган по въпроси, свързани с обработването, и да се консултира с надзорния орган по всякакви въпроси свързани с обработването на лични данни за нуждите на Центъра.

❖ Длъжностното лице по защита на данните има право:
- Да събира информация за определяне на дейностите по обработване и да получава необходимото съдействие и информация от страна на ръководството на центъра, от обработващите лични данни и от другите релевантни отдели и структури, имащи отношение към операциите по обработване на лични данни;
- Да анализира и проверява изпълнението на дейностите по обработване;
- Да съветва, информира и да дава препоръки на администратора и обработващите лични данни;
- При изпълнение на своите задачи ДЛЗД действа напълно независимо и свободно от указанията на администратора.

❖ Служителите на ЦСОП са длъжни:
- Да обработват лични данни законосъобразно, добросъвестно и прозрачно;
- Да използват личните данни, до които имат достъп, съобразно целите, за които се събират, и да не ги обработват допълнително по начин, несъвместим с тези цели;
- Да актуализират регистрите на лични данни при необходимост;
- Да поддържат личните данни във вид, който позволява идентифициране на съответните физически лица, за период не по – дълъг от необходимия за целите, за които тези данни се обработват;
- Да заличават или коригират личните данни когато се установи, че са неточни или непропорционални по отношение на целите, за които се обработват;
- Да пазят в поверителност и да не разгласяват лични данни, до които са получили достъп при или по повод изпълнение на задълженията си;
- Незабавно да уведомяват администратора на лични данни и ДЛЗД в случай, че установят изтичане на лични данни, независимо дали при извършване на своята лична работа или на работата на друго лице, обработващо лични данни.

Ако в резултат на действията на съответен служител по обработване на лични данни са произтекли вреди за трето лице, същото може да потърси отговорност по реда на общото гражданско законодателство или по наказателен ред.

Чл.15. Права на физическите лица – субекти на данни:

❖ **Право на достъп на субекта на данните**

Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

- целите на обработването;
- съответните категории лични данни;
- получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни;

- предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;
- съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване; правото на жалба до надзорен орган;
- когато личните данни не са събрани от субекта на данните - всякаква налична информация за техния източник.

❖ **Право на коригиране**

Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните или непълни лични данни, свързани с него, предвид целите на обработването.

❖ **Право на изтриване (реализиране на правото „да бъдеш забравен“)**

- Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни, а администраторът има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от посочените по-долу основания:
- личните данни повече не са необходими за целите, за които са били събрани или обработвани;
- субектът на данните оттегли своето съгласие, върху което се основава обработването на данните;
- субектът на данните възразява срещу обработването.

❖ **Право на ограничаване на обработването**

Субектът на данните има право да изиска от администратора ограничаване на обработването в законоустановени случаи. Когато субект на данните е изискал ограничаване на обработването, администраторът го информира преди отмяната на ограничаването на обработването.

Администраторът съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки субект, освен ако това е невъзможно или изисква несъразмерно големи усилия.

❖ **Право на преносимост на данните**

Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени първоначално.

❖ **Право на възражение**

Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на неговите лични данни. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта, или че е необходимо за установяването, упражняването или защитата на правни претенции.

Искания на субектите на данни във връзка с техните права се приемат от администратора по следните начини:

- На адреса на администратора: с. Кривня, ул. Първа № 1

- По електронната поща на адрес: info-400162@edu.mon.bg

Редът за упражняване на горните права от физическите лица – субекти на данни и за подаване на искания до администратора е подробно описан в **Инструкция за подаване и приемане на заявления за достъп, коригиране, изтриване и ограничено обработване на лични данни**, представляваща приложение към настоящия правилник. Исканията до администратора се подават чрез Заявление по образец, приложен в Инструкцията.

Отговор на искането се предоставя от администратора без ненужно забавяне, най-късно в рамките на **1 (един) месец** от получаване на искането. Отговорът се дава в същата форма, в която е отправено искането т.е. на искания отправени по електронен път се отговаря по електронен път, а на искания отправени на хартиен носител до адрес на институцията се отговаря в писмена форма на хартиен носител до адрес на субекта на данни, освен ако субектът на данни не е поискал друго.

Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с полученото от него искане. Когато администраторът има основателни опасения във връзка със самоличността на лицето, което е подало искане, той изисква предоставяне на допълнителна информация, необходима за потвърждаване на самоличността на субекта. В случай, че администраторът възнамерява да не уважи подаденото искане, той посочва причините за това.

При получаване от администратора на жалби от физически лица с претенции за нарушаване изискванията на Регламента от негова страна, при получаване на искания за обезщетения, както и каквито и да е отправени указания, предупреждения, разпореждания и наложени санкции от надзорния орган, те се предават незабавно на длъжностното лице по защита на данните, назначено от администратора, за становище и изготвяне на доклад до директора на центъра. След преглед на доклада директорът прави преценка за подходящите действия, които да бъдат предприети.

Чл.16. Ред за уведомяване на надзорния орган и на субекта на данни за нарушение на сигурността на личните данни:

Нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен начин, да доведе до физически, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица.

Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми надзорния орган (**Комисията за защита на личните данни**) за нарушението на сигурността на личните данни без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, освен ако администраторът не е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и че информацията може да се подаде поетапно без ненужно допълнително забавяне.

В уведомлението се съдържа най-малко следното:

- описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;
- посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Администраторът следва да уведоми и субекта на данни за нарушението на сигурността на личните данни без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице, за да му се даде възможност да предприеме необходимите предпазни мерки. В уведомлението следва да се посочва естеството на нарушението на сигурността на личните данни, както и да се дадат препоръки на засегнатото физическо лице за това как да ограничи потенциалните неблагоприятни последици.

ИНФОРМАЦИЯ ЗА НАДЗОРНИЯ ОРГАН:

Комисия за защита на личните данни

Адрес: гр. София, п.к. 1784, бул. „проф. Цветан Лазаров“ № 2

Център за информация и контакти - тел: 02/91-53-518

Приемна - работно време 9:00 - 17:30 ч.

Електронна поща: kzld@cpdp.bg

Интернет страница: www.cpdp.bg

Чл.17. Правомощия на надзорния орган и налагани от него санкции

За нарушения на Регламента надзорния орган има право да налага административни наказания „глоба“ или „имуществена санкция“. Видът на наказанието и неговият размер се определят от надзорния орган във всеки отделен случай, като се вземат предвид всички обстоятелства, свързани с конкретната ситуация, по-специално при надлежно отчитане на естеството, тежестта и продължителността на нарушението и на последиците от него, както и на мерките, предприети, за да се гарантира спазване на задълженията по Регламента и за да се предотвратят или смекчат последиците от нарушението.

Освен да налага административни наказания „глоба“ или „имуществена санкция“, надзорния орган има и следните корективни правомощия: да отправя предупреждения и официални предупреждения до администратора или обработващия лични данни, да отправя разпореждания за изпълнение по определен начин и в определен срок, да налага временно или окончателно ограничаване на обработването на данни, да разпорежда коригиране, изтриване на лични данни или ограничаване на обработването им.

Надзорният орган КЗЛД има правомощие да провежда разследвания под формата на одити във връзка със защита на данните, във връзка с което има право на достъп до всички помещения на

администратора и обработващия лични данни, до цялото оборудване и технически средства за обработване. Надзорният орган има право да изисква от администратора и обработващия лични данни всички данни и цялата информация, от която се нуждае за изпълнение на своите задачи.

Чл.18. Политики, процедури и правила приложими при предоставяне на лични данни от институцията на трети лица:

Лични данни се предоставят от администратора на трети лица в следните хипотези:

- Когато това е задължително по закон, свързано е с изпълнение на законови задължения на администратора или е изрично изискано от публичен орган (централен или местен регулаторен орган) в рамките на упражняване на негови законови правомощия;
- Когато това е необходимо за дейността на администратора, единствено след получаване на писмена декларация от третото лице, че дейността му е приведена в съответствие с изискванията на Регламента.

РАЗДЕЛ. 3

ПРЕХОДНИ И ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

- 1. Всички служители и специалисти в ЦСОП“ Св. св Кирил и Методий“ са длъжни срещу подпис да се запознаят с настоящите вътрешни правила за защита на личните данни и да ги спазват.
- 2. Вътрешните правила се издават на основание на Закона за защита на личните данни и Регламент (ЕС) 2016/679.
- 3. За всички неуредени в настоящите вътрешни правила въпроси се прилагат разпоредбите на Регламент (ЕС) 2016/679, Закона за защита на личните данни и действащото приложимо законодателство на Република България.
- 4. Вътрешните правила се утвърждават със Заповед на Директора на ЦСОП с. Кривня

Приложения:

1/ Процедура по обработване, съхранение и защита на лични данни при видеонаблюдение в ЦСОП“ Св. св Кирил и Методий“;

2/ Инструкция за подаване и приемане на заявления за достъп, коригиране, изтриване и ограничено обработване на лични данни;

3/ Формуляр за предоставяне на съгласие от субекта на данни;

4/ Формуляр за оттегляне на съгласие от субекта на данни.